IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MASSACHUSETTS

ALLIANCE FOR AUTOMOTIVE INNOVATION Plaintiff, vs. MAURA HEALEY, ATTORNEY GENERAL OF THE COMMONWEALTH OF MASSACHUSETTS in her official capacity, Defendant.	C.A. No. 1:20-cv-12090

Declaration of John Robb

1. I am currently employed by Hyundai America Technical Center, Inc. ("HATCI"). HATCI serves as the local in-market R&D center for Kia Motors Corporation ("KMC") assisting in research and development of all Kia-branded vehicles sold by Kia Motors America, Inc. ("KMA") in the United States (collective organization referred to as "Kia" herein). I have been employed by HATCI since June 2, 2008. I currently serve as the Director of Electronic Systems Development and I am responsible for North American market integration, development, and validation for vehicle infotainment, active safety, and cybersecurity electronic control units ("ECU") for all KMA vehicles. This declaration is based on my personal knowledge.

2. As the Director of Electronic Systems Development for HATCI, I have been involved in the development and testing process for all Kia vehicles currently offered for sale on dealership lots, as well as the vehicles Kia will offer for sale as Model Year 2022 vehicles. Kia has completed or is in process of development and testing for Model Year 2022 vehicles. This

includes conducting the initial validation and final quality validation, and monitoring the testing program to ensure vehicle quality and reliability.

3. Focusing on the vehicle Electronic Control Units, there are broadly five disciplines of development for vehicle integration: (1) Hardware development; (2) Vehicle integration and packaging; (3) Software development; (4) Communication development; and, (5) Off-board server and application system development and integration. In general, the development lead-time for new ECUs is approximately 30-42 months, while development of carryover systems in new vehicles can take 24-30 months. Development of these ECUs and related systems integrate multiple functions across the organization and require involvement of Research and Development, Manufacturing, Quality, Sales, Marketing, Security, and Legal, among others. In my estimation, it costs millions of dollars to perform new ECU development and billions for the entire vehicle.

4. Kia takes seriously the design, implementation, and maintenance of secure vehicle systems and vehicle data. Kia protects its vehicle systems and onboard vehicle data with a variety of access controls. These access controls help to ensure the security, safety, and performance of Kia's vehicles, as well as protect Kia's intellectual property in its vehicle systems.

5. In addition to the development and implementation teams that support vehicle security, Kia's access controls are designed and maintained by a team of dozens of dedicated cybersecurity specialists working in the United States and globally across the Kia organization.

6. Kia controls access to its vehicle systems, including in particular the firmware that executes core vehicle functions such as steering, acceleration, braking, and airbags. These

access controls help to ensure that access to vehicle systems involving core vehicle functions are limited to those with Kia's authorization.

7. Kia's access controls around vehicle systems include encryption keys, unique IDs, password protections, asymmetric keys exchanged between vehicle systems and a member's servers, authorized message requirements, secure boot, secure storage, network domain segregations, public key infrastructures to scribe digital signatures, hashing algorithm and paired public and private key topology, cellular secure protocols, and firewalls designed to control and protect the flow of messages in vehicle systems. One such system in place across multiple vehicle models is the secure central gateway, which serves as a Connectivity Control Unit for all communications to the vehicle network through the OBD-II port. Full access to the vehicle network beyond this gateway requires authorization using approved access credentials, including password, and an asymmetric key. To comply with the existing Right to Repair framework, this authorization is available to any trusted source, including vehicle owners and repair shop technicians.

8. As part of its system of access and security controls, Kia has begun to deploy measures to all new model refreshes that ensure the logical and physical isolation of vehicle control systems from external connections to provide layers of protection for any cybersecurity threats, consistent with federal cybersecurity guidance. Moreover, Kia is deploying security measures that detect intrusions and threats (Intrusion Detection System, or "IDS") to future new models. This system will identify abnormal behavior and anomalies within the system architecture. Future design processes will apply security measures that report these to a security operations center, which will then make a decision to disable or prevent access of the anomaly into the vehicle without affecting vehicle safety controls (Intrusion Detection and Prevention

System, or "IDPS"). By doing so, Kia helps to prevent access, or mitigate the risks of any access, by unauthorized third parties to core vehicle functions, including the ability remotely to take control of vehicles. Kia has worked to build these and other security layers into its safety systems at the direction of the National Highway Traffic Safety Administration (NHTSA). *See* NHTSA, *Cybersecurity Best Practices for Modern Vehicles* (Oct. 2016).

9. By requiring the creation of an "open access" platform with read/write capabilities, the data law that Massachusetts voters passed on November 3, 2020 as Proposition 1 (the "Data Law") makes Kia's extensive efforts to design and maintain secure, segregated vehicle systems far more challenging. Based on my 25 years of experience in military and automotive vehicle electronics development, a remotely accessible system with read/write capabilities—particularly one that is standardized across vehicle models or across the entire industry—would greatly increase the risk of cybersecurity threats and the severity of any cybersecurity attacks by making vehicle systems easier for hackers to penetrate and allowing any hackers who do access vehicle systems greater ability to compromise core vehicle functions such as steering, acceleration, braking, and air bags.

10. Allowing third-party read/write access to vehicle systems without manufacturer authorization would threaten the integrity of vehicle systems and the safe operation of vehicles by opening access to both hackers and mechanics making inadvertent changes without appreciating the significant impact those changes can have.

11. I am not aware of any currently existing system architecture that would satisfy the Data Law requirements for an "open access" platform with read/write capabilities that is standardized across all makes and models, either within a manufacturer or across the industry.

12. Any action that removes or limits the operability of existing access controls around vehicle systems necessarily leaves vehicles more vulnerable to a cyberattack and increases the potential severity of any cyberattack.

13. Kia uses a variety of proprietary elements in the design of their vehicle systems. These include, but are not limited to, source and object code; distinctive screen layouts; graphical content; text arrangement, organization, and the display of information; ride and handling algorithms; active and passive safety performance firmware; and dynamic user experience (voice recognition and prompts). These elements are applied to each vehicle in a unique manner based upon Kia's brand expectations and vehicle business case. Each system shall comply with Kia's safety and security protocols, quality and reliability requirements and compliance to driver's distraction policies.

14. Kia utilizes proprietary component firmware, software, and configuration files across its vehicle systems. These solutions are designed in-house by affiliates within the Hyundai Motor Group, of which Kia is a part, and are not shared with or sold to other automotive manufacturers. They are the product of millions of dollars of research and countless hours of development for the sole and exclusive use in vehicles manufactured by companies within the Hyundai Motor Group. For example, Electronic Control Units on the vehicle network communicate to each other in a proprietary fashion using an internally developed set of controls. The content of the messages sent along the network are unique to each make and model.

15. The Data Law requires an extensive and costly modification of vehicle systems and the creation of an entirely new platform architecture for accessing vehicle data. Kia would have to begin work (and begin incurring significant costs) immediately. Even if it were possible to create the vehicle systems and platforms contemplated by the Data Law, it would not be

possible to do so in the Data Law's timeframe. It will take years of labor at extensive cost to design, test, implement, and standardize across all models a new vehicle platform architecture.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed on: November 30, 2020

John Robert Robb
John Robert Robb (Dec 1, 2020 09:56 EST)

John Robb